

Quantum Noise Control

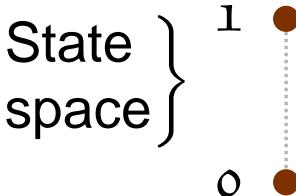
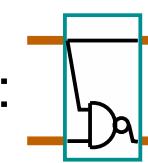
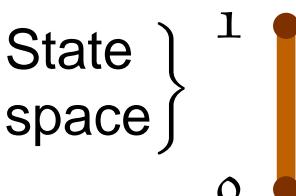
Algebraic Methods

Manny

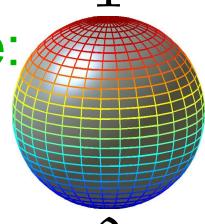
- Subsystems for quantum information.
- Models of quantum noise.
- Codes for general noise.
- Clifford codes.

knill@lanl.gov, <http://www.lanl.gov/~knill>

Information Processing Theories

	Information Unit	Combining Units	Operations	Readout
Classical:	<p>Bit</p> <p>State space } $\begin{matrix} 1 \\ 0 \end{matrix}$</p> 	<p>Concatenation</p> <p>Product space: 0000 1101 ...</p>	<p>“New bit”</p> <p>nand:</p>  <p>Repetition</p>	<p>NA</p> 
Probabilistic:	<p>P-Bit</p> <p>State space } $\begin{matrix} 1 \\ 0 \end{matrix}$</p> <p>$\{p:0; (1-p):1\}$</p> 	<p>Convex combination of products</p>	<p>Classical ops</p> <p>“Coin toss”</p>	<p>Conditioning</p>

Information Processing Theories

	Information Unit	Combining Units	Operations	Readout
Quantum: Pure state:	<p>Qubit</p> <p>Hilbert space:</p>  <p>$\alpha 0\rangle + \beta 1\rangle \in \mathbb{C}^2$</p> <p>$\mapsto \mathbb{CP}_1$</p>	<p>Tensor product</p> <p>$\alpha 00\rangle + \beta 01\rangle +$</p> <p>$\in \mathbb{C}^2 \otimes \mathbb{C}^2$</p> <p>$\mapsto \mathbb{CP}_3$</p>	<p>“New qubit”</p> <p>2-qubit unitary</p>	<p>Measurement</p> <p>\Rightarrow “Collapse”</p>
Mixed state:	<p>Probabilistic combinations</p> <p>+ {super-position principle}</p>	<p>Bit states</p>	<p>discard</p> <p>reset</p> <p>Condition on pbit</p>	<p>To pbit ...</p>

Realizing Quantum Information

Is quantum information physically realizable?

- **Accuracy Threshold Theorem 1:**

Assume the *requirements for scalable computing*. If the error per gate (including “no-op”) is less than a threshold, then it is possible to efficiently quantum compute arbitrarily accurately.

Shor 1996[1], Kitaev 1996[2], Aharonov&Ben-Or 1996[3], Knill & al. 1996[4].

Finite Quantum Systems I

A finite quantum system Q is determined by:

- A Hilbert space \mathcal{Q} .
 - $\dim \mathcal{Q} = N$.
 - “Logical” orthonormal basis: e_1, \dots, e_N .
 - Unit vectors of \mathcal{Q}
 - \mapsto pure states of Q .

Examples ($N = 2$):

$$\begin{aligned}\langle i e_1 | .6 e_1 + .8 e_2 \rangle &= (i e_1)^* (.6 e_1 + .8 e_2) \\ &= \begin{pmatrix} -i & 0 \end{pmatrix} \begin{pmatrix} .6 \\ .8 \end{pmatrix} \\ &= -.6 i\end{aligned}$$

- Probability distributions over unit vectors of \mathcal{Q}
 - \mapsto mixed states of Q .

Finite Quantum Systems II

A finite quantum system Q is determined by:

- A $*$ -algebra of “observables” $\mathcal{A}_Q \simeq \text{Mat}_N(\mathbb{C})$.
 - States are positive linear functionals:

$$\begin{aligned} A &\rightarrow \langle A \rangle_\rho \in \mathbb{C} \\ \langle A^* A \rangle_\rho &\geq 0 \\ \langle \mathbb{I} \rangle_\rho &= 1 \end{aligned}$$

- States are convex-closed.
- Pure states = extreme points.

Examples ($N = 2$): $\text{Mat}_2(\mathbb{C})$ acts on \mathbb{C}^2 .

Unit vector in \mathbb{C}^2 determines pure state:

$$\left\langle \begin{pmatrix} .5 & i \\ 0 & .2 \end{pmatrix} \right\rangle_{e_2} = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} .5 & i \\ 0 & .2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = .2$$

Quantum Subsystems



- Sets of pure states:

$$\mathcal{Q}$$

$$\mathcal{Q} \otimes \mathcal{Q}$$

- A subsystem's Hilbert space:

Factor of a subspace

- Observable algebras:

$$\text{Mat}_2(\mathbb{C}) \simeq \text{Mat}_2(\mathbb{C}) \otimes \mathbb{I} \quad \subseteq \quad \text{Mat}_4(\mathbb{C})$$

- A subsystem's observables:

Sub-*-algebra $\simeq \text{Mat}_n(\mathbb{C})$

Math Objects and Tools

- Hilbert spaces.
 - $*$ -algebras and positive linear forms.
 - Representations of $*$ -algebras.
- **Theorem 2:** Let \mathcal{A} be an algebra of complex matrices acting irreducibly on \mathbb{C}^n . Then $\mathcal{A} = \text{Mat}_n(\mathbb{C})$. Burnside
- **Theorem 3:** Let \mathcal{A} be a $*$ -subalgebra of $\text{Mat}_N(\mathbb{C})$ with $\mathcal{A} \simeq \text{Mat}_n(\mathbb{C})$. Then there is a unitary map

$$U : \mathbb{C}^N \rightarrow \mathbb{C}^n \otimes \mathbb{C}^s \oplus \mathbb{C}^r$$

such that

$$U\mathcal{A}U^* = \text{Mat}_n(\mathbb{C}) \otimes \mathbb{I}_s \oplus \mathbb{O}_r$$

See for example Burrow [5]

Subsystems from Algebras

- **Theorem 4:** Let \mathcal{A} be a $*$ -subalgebra of $\text{Mat}_N(\mathbb{C})$. Let \mathcal{A}' be the commutant of \mathcal{A} . Then there is a unitary map

$$\begin{aligned} U : \mathbb{C}^N &\rightarrow \mathbb{C}^{n_1} \otimes \mathbb{C}^{s_1} \oplus \mathbb{C}^{n_2} \otimes \mathbb{C}^{s_2} \\ &\quad \vdots \\ &\quad \oplus \mathbb{C}^{n_k} \otimes \mathbb{C}^{s_k} \end{aligned}$$

such that

$$\begin{aligned} U\mathcal{A}U^* &= \text{Mat}_{n_1}(\mathbb{C}) \otimes \mathbb{I}_{s_1} \oplus \text{Mat}_{n_2}(\mathbb{C}) \otimes \mathbb{I}_{s_2} \\ &\quad \vdots \\ &\quad \oplus \text{Mat}_{n_k}(\mathbb{C}) \otimes \mathbb{I}_{s_k} \end{aligned}$$

and

$$\begin{aligned} U\mathcal{A}'U^* &= \mathbb{I}_{n_1} \otimes \text{Mat}_{s_1}(\mathbb{C}) \oplus \mathbb{I}_{n_2} \otimes \text{Mat}_{s_2}(\mathbb{C}) \\ &\quad \vdots \\ &\quad \oplus \mathbb{I}_{n_k} \otimes \text{Mat}_{s_k}(\mathbb{C}) \end{aligned}$$

A Classical Error Model

- $\{ \text{000}, \text{001}, \dots, \text{111} \}$: A finite classical system.

- Bit flip errors, X_i :

$$X_2(\text{011}) = \text{0}\cancel{\text{0}}\text{1}.$$

- Weight one errors:

$$\mathcal{X}_1 = \{X_1, X_2, X_3\}.$$

- Weight two errors:

$$\mathcal{X}_2 = \{X_1X_2, X_1X_3, X_2X_3\}.$$

- + superpositions \rightarrow quantum system, error model.

Error Algebras

- Q : Quantum system.
- $\mathcal{A}_Q \simeq \text{Mat}_N(\mathbb{C})$: Its observable algebra acting on...
- \mathcal{Q} : Its Hilbert space of pure states.
- Effect of noise: $E \in \mathcal{A}_Q$.

$$\psi \rightarrow E\psi$$

- Weight one errors: $\mathcal{E}_1 \subseteq \mathcal{A}_Q$, linearly closed set, $\mathbb{I}_Q \in \mathcal{E}_1$.
- Weight $\leq k$ errors: $\mathcal{E}_k = \mathcal{E}_1^k$.
- Error algebra $\mathcal{E} = \mathcal{E}_\infty$:

$$\mathcal{E}_0 = \text{span } \mathbb{I}_Q \subseteq \mathcal{E}_1 \subseteq \mathcal{E}_2 \subseteq \dots \subseteq \mathcal{E}$$

Knill&Laflamme&Viola 1999 [6]

A Typical Noiseless Subsystem

- System: $\mathcal{C} = \{ 000, 001, \dots, 111 \}$.
Errors: $\mathcal{X}_1 = \{ X_2, X_3 \}$.

Problem: How to protect one bit?

Solution: Place the bit's state in the first bit of C.

$$\alpha e_0 + \beta e_1 \rightarrow (\alpha e_0 + \beta e_1) \otimes e_{00} \xrightarrow{X_2^2} (\alpha e_0 + \beta e_1) \otimes e_{10}$$

$$\xrightarrow{X_3^3} (\alpha e_0 + \beta e_1) \otimes e_{01}$$

$$\xrightarrow{X_2 X_3} (\alpha e_0 + \beta e_1) \otimes e_{11}$$

Noiseless Subsystems

- Let subsystem S be defined by the *-subalgebra $\mathcal{A}_S \subseteq \mathcal{A}_Q$ associated with the factorization

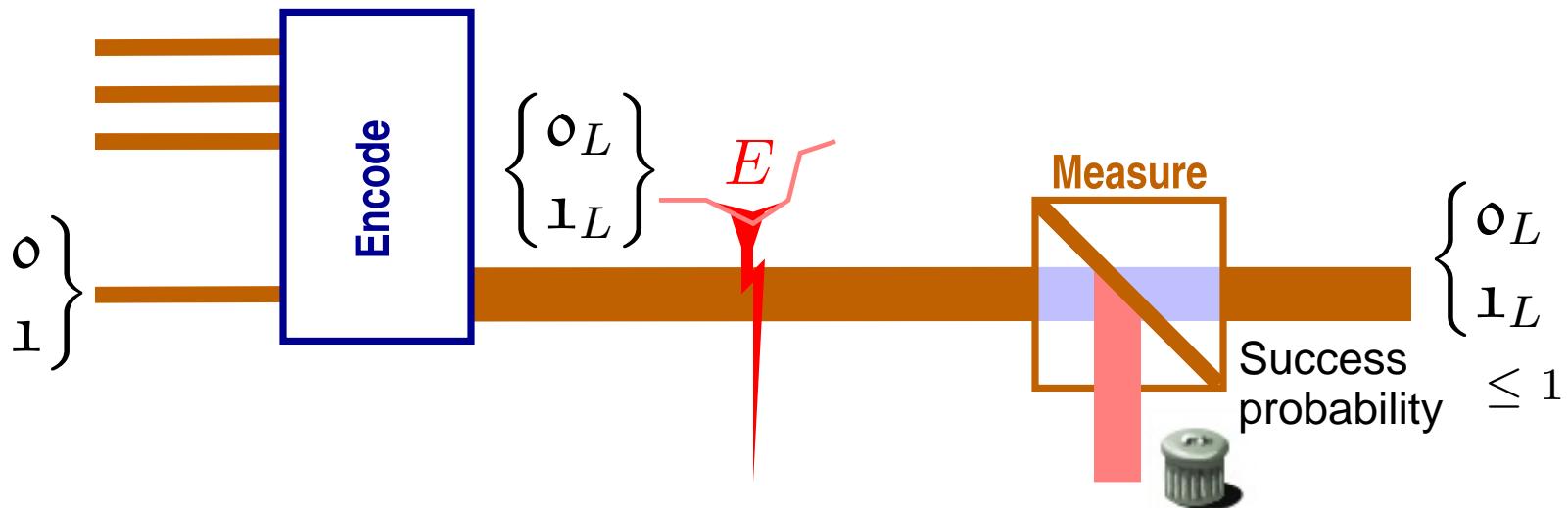
$$\mathcal{Q} \xrightarrow{U} \mathbb{C}^s \otimes \mathbb{C}^t \oplus \mathbb{C}^r$$

- Theorem 5:** The following are equivalent:
 - For every $E \in \mathcal{E}$,
- $$UEU^\dagger \in \mathbb{I}_s \otimes \text{Mat}_t(\mathbb{C}) \oplus \text{Mat}_r(\mathbb{C})$$
- \mathcal{E} is a subset of the commutant of \mathcal{A}_S .

Proof. By Thm. 4.

- Definition:** A subsystem satisfying 1 or 2 is called *noiseless for \mathcal{E}* .

Classical Error Detection



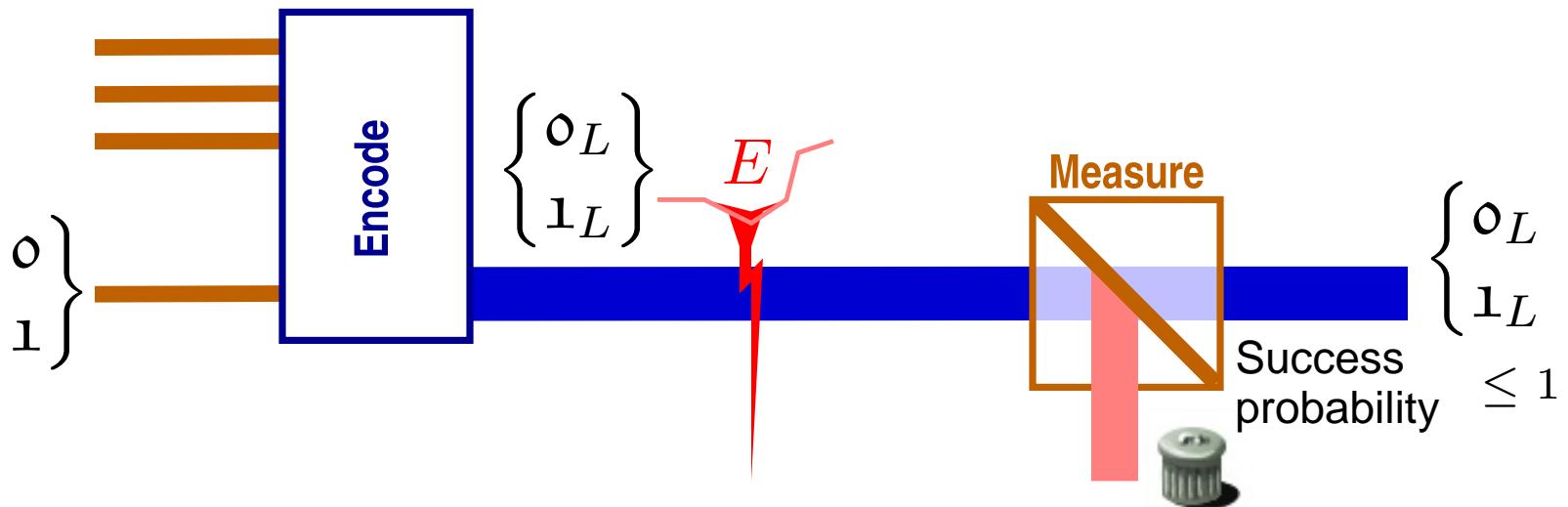
Codewords: $\begin{cases} o_L = 00 \\ 1_L = 11 \end{cases}$

$\xrightarrow{\mathbb{I}} \begin{cases} 00 \\ 11 \end{cases}$ Still in code? —Yes.

$\xrightarrow{X_1} \begin{cases} 10 \\ 01 \end{cases}$ —No.

$\xrightarrow{X_1 X_2} \begin{cases} 11 \\ 00 \end{cases}$ —Yes.

Classical Error Detection



Quantum channel:

Project onto
 $\text{span}(e_{00}, e_{11})$
with P_C .

$$\begin{cases} 0_L = e_{00} \\ 1_L = e_{11} \end{cases} \xrightarrow{\mathbb{I}} \begin{cases} e_{00} \\ e_{11} \end{cases} \quad \begin{cases} P_C e_{00} = e_{00} \\ P_C e_{11} = e_{11} \end{cases}$$
$$\xrightarrow{X_1} \begin{cases} e_{10} \\ e_{01} \end{cases} \quad \begin{cases} P_C e_{10} = 0 \\ P_C e_{01} = 0 \end{cases}$$

Error-detecting C-Codes

- **Definition:** A c -code of \mathcal{Q} is an orthonormal sequence of vectors $\mathcal{C} = (c_1, \dots, c_n) \subseteq \mathcal{Q}$.
 - Encode symbol i as c_i .
- **Definition:** \mathcal{C} detects E if
For all $i \neq j$: $c_i^* E c_j = 0$.

- Equivalently:

$$E = \left(\begin{array}{cccc} & \overbrace{\quad \quad \quad \quad}^{\mathcal{C}} & & \\ \mathcal{C} \left\{ \begin{array}{cccc} \lambda_{1,E} & 0 & \dots & 0 \\ 0 & \lambda_{2,E} & & \vdots \\ \vdots & & \ddots & \\ 0 & & \dots & \lambda_{n,E} \end{array} \right. & & E_{12} & \\ & E_{21} & & E_{22} \end{array} \right)$$

Existence of Good C-Codes

- Let \mathcal{E}_d be a t -dimensional subspace of error operators.
- Theorem 6:** There exists an \mathcal{E}_d -detecting c-code of size $\geq N/t$.

Proof:

1. Pick a unit $c_1 \in \mathcal{Q}$.

2. Inductively:

$$P_k = (\mathcal{E}_d \text{ span}(c_1, \dots, c_k))^{\perp}.$$

Pick $c_{k+1} \in P_k^{\perp}$. Possible if $\dim P_k < N$.

3. Observe that $\dim P_k \leq kt$.

- Problem 7:** What is the minimum size $C(t, N)$ of the largest \mathcal{E}_d -detecting c-code?

Thm. 6: $C(t, N) \geq N/t$.

Error-detecting Q-Codes

- **Definition:** A q -code of \mathcal{Q} is a subspace $\mathcal{S} \subseteq \mathcal{Q}$ ($n \doteq \dim \mathcal{S}$).
 - Encode state ψ unitarily to $U\psi \in \mathcal{S}$.
- **Definition:** \mathcal{S} detects E if
 - For all $\psi \perp \phi \in \mathcal{S}$ $\psi^* E \phi = 0$.
- Equivalently: Let $P_{\mathcal{S}}$ be the projection onto \mathcal{S} .

$$P_{\mathcal{S}} E P_{\mathcal{S}} = \lambda_E P_{\mathcal{S}}.$$

- Equivalently:

$$E = \left(\begin{array}{cccccc} & & \overbrace{\mathcal{S}} & & & \\ \lambda_E & 0 & \dots & 0 & & \\ 0 & \lambda_E & & & & \\ \vdots & & \ddots & & & \\ 0 & & \dots & \lambda_E & & \\ & & & & E_{12} & \\ & & & & E_{21} & \\ & & & & & E_{22} \end{array} \right)$$

Existence of Good Q-Codes

- Let \mathcal{E}_d be a t -dimensional subspace of error operators and \mathcal{C} a size k c-code.
- Theorem 8:** There exists an \mathcal{E}_d -detecting q-code $\mathcal{S} \subseteq \text{span } \mathcal{C}$ of dimension $\geq k/(t + 1)$.

Proof: Based on a convex intersection argument.
See [7, 6].

- Corollary 9:** . There exists an \mathcal{E}_d -detecting q-code of dimension $\geq N/(t(t + 1))$.
- Problem 10:** What is the minimum size $Q(t, N)$ of the largest \mathcal{E}_d -detecting q-code?

Cor. 9: $Q(t, N) \geq N/(t(t + 1))$.

From Error Detection to Error Correction

- Error algebra:

$$\mathcal{E}_\infty \supseteq \dots \supseteq \mathcal{E}_2 = \mathcal{E}_1 \mathcal{E}_1 \supseteq \mathcal{E}_1 \supseteq \mathcal{E}_0 = \text{span } \mathbb{I}_Q.$$

- **Definition:** A $(c|q)$ -code has *minimum distance* d for \mathcal{E}_1 if it detects \mathcal{E}_{d-1} .
- **Theorem 11:** A minimum distance $2e + 1$ $(c|q)$ -code can be used to correct up to e errors (any error in \mathcal{E}_e).

Bennett&*al.* 1996 [8], Knill&Laflamme 1996 [9], Knill&Laflamme&Viola 1999 [6],
General reference: (M)ike 2001 [10]

Group Codes I

- G A group.
 $\pi : G \rightarrow \text{Mat}_N(\mathbb{C})$
 $\pi : g \mapsto \pi_g$ } Unitary, faithful irrep.
- Subspaces via irreps of subgroups:
 - Let $H \subseteq G$ be a subgroup, χ_i irreps occurring in $\pi \upharpoonright H$.

$$\pi : H \rightarrow \begin{pmatrix} \boxed{\chi_1} \otimes \mathbb{I}_c & 0 & \dots \\ 0 & \boxed{\chi_2} \otimes \mathbb{I}_c & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

- Projection onto the block for $\chi_i \otimes \mathbb{I}_c$:

$$P_{\chi_i} \propto \sum_{h \in H} \bar{\chi}_i(h) \pi_h.$$

Knill 1996 [11, 12]

Group Codes II

- $\pi : g \mapsto \pi_g$ a unitary, faithful irrep of group G .
- Let $H < G$ be a normal subgroup, χ one of the irreps occurring in $\pi \upharpoonright H$, $Z(H)$ the center of H .

Define: $\chi^g : h \mapsto \chi(ghg^{-1})$.

$$\chi^\perp = \{g \in G : \chi^g = \chi\}.$$

χ^\perp is the *inertia* subgroup of χ , $H \subseteq \chi^\perp$.

- **Theorem 12:** Let $\mathcal{S} = \text{rng}(P_\chi)$. Then $\dim(\mathcal{S}) = |G/\chi^\perp|$ and \mathcal{S} detects every operator of $\pi(G)$ *not* in $\pi(\chi^\perp \setminus Z(H))$.

Proof:

1. $\dim \chi^g = \dim \chi$, $\chi_i = \chi^{g_i}$ for some g_i .
2. $g \in Z(H)$: $\pi_g \upharpoonright \mathcal{S} = e^{i\phi} \mathbb{I}_{\mathcal{S}}$ for some ϕ .
3. $g \notin \chi^\perp$: $\pi_g \mathcal{S} \perp \mathcal{S}$, since π_g permutes the irreps of H .

Classes of Group Codes

- Clifford Codes: Klappenecker&Roetteler 2001 [13]
 1. π is induced by a projective representation of $\tilde{G} = G/Z(G)$.
 2. Minimality: $|\tilde{G}| = N^2$.
 - **Theorem 13:** G is solvable. Klappenecker&Roetteler 2001 [14]
- Stabilizer Codes:
Clifford code with χ (irrep of $H < G$) one-dimensional.
Gottesman 1996 [15], Klappenecker&Roetteler 2001 [13]
- $\text{GF}_{p^{2n}}$ codes.
Stabilizer Codes with $\tilde{G} \simeq (\text{GF}_p)^{2n}$.
Calderbank&*al.* 1996 [16], Rains 1997 [17]
Ashikhmin&Knill 2000 [18]

Conclusion and Open Problems

- **Problem 7:** What is the minimum size $C(t, N)$ of the largest \mathcal{E} -detecting c-code?

Thm. 6: $C(t, N) \geq N/t.$

- **Problem 10:** What is the minimum size $Q(t, N)$ of the largest \mathcal{E} -detecting q-code?

Cor. 9: $Q(t, N) \geq N/(t(t + 1)).$

- **Question 14:** Is it possible to construct “good” group, non-GF _{q^2} codes for physically relevant error models?

Contents

Title: Quantum Noise Control	0	Classical Error Detection	13
Information Processing Theories	1	Classical Error Detection	14
Information Processing Theories	2	Error-detecting C-Codes	15
Realizing Quantum Information	3	Existence of Good C-Codes	16
Finite Quantum Systems I	4	Error-detecting Q-Codes	17
Finite Quantum Systems II	5	Existence of Good Q-Codes	18
Quantum Subsystems	6	From Error Detection to Error Correction	19
Math Objects and Tools	7	Group Codes I	20
Subsystems from Algebras	8	Group Codes II	21
A Classical Error Model	9	Classes of Group Codes	22
Error Algebras	10	Conclusion and Open Problems	23
A Typical Noiseless Subsystem	11	References	25
Noiseless Subsystems	12		

References

- [1] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Symposium on the Foundations of Computer Science (FOCS)*, pages 56–65, Los Alamitos, California, 1996. IEEE press.
- [2] A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52:1191–1249, 1997.
- [3] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)*, pages 176–188, New York, New York, 1996. ACM Press.
- [4] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279:342–345, 1998.
- [5] M. Burrow. *Representation Theory of Finite Groups*. Academic Press, New York, 1965.
- [6] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.
- [7] H. Tverberg. A generalization of radon’s theorem. *J. London Math. Soc.*, 41:123–128, 1966.
- [8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error-correcting codes. *Phys. Rev. A*, 54:3824–3851, 1996.
- [9] E. Knill and R. Laflamme. A theory of quantum error correcting codes. *Phys. Rev. A*, 55:900–911, 1997.
- [10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2001.
- [11] E. Knill. Non-binary unitary error bases and quantum codes. Technical Report LAUR-96-2717, Los Alamos National Laboratory, knill@lanl.gov, 1996. quant-ph/9608048.
- [12] E. Knill. Group representations, error bases and quantum codes. Technical Report LAUR-96-2807, Los Alamos National Laboratory, <http://www.c3.lanl.gov/~knill>, 1996. quant-ph/9608049.
- [13] A. Klappenecker and M. Roetteler. Beyond stabilizer codes. quant-ph/0010076, 2001.
- [14] A. Klappenecker and M. Roetteler. A remark on unitary error bases. quant-ph/0010082, 2001.
- [15] D. Gottesman. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.
- [16] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. A*, 78:405–408, 1997.
- [17] E. R. Rains. Nonbinary quantum codes. quant-ph/9703048, 1997.
- [18] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. quant-ph/0005008, to appear in *IEEE Tr. Inf. Th.*, 2000.